

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-036383

(43)Date of publication of application : 07.02.1995

(51)Int.Cl.

G09C 5/00

G06K 7/10

G06K 17/00

(21)Application number : 05-315847

(71)Applicant : PITNEY BOWES INC

(22)Date of filing : 22.11.1993

(72)Inventor : MARCUS JAMES R

(30)Priority

Priority number : 92 979018 Priority date : 20.11.1992 Priority country : US

(54)METHOD FOR IDENTIFYING OBJECT AND OTHER ENTITY AND DEVICE FOR
MANUFACTURING IDENTIFICATION CARD

(57)Abstract:

PURPOSE: To obtain an identification card which is safe
against alteration and forgery.

CONSTITUTION: A digital signal generated by scanning an
entity to be certified by an identification card, is compressed
(16), enciphered (20), encoded as a two-dimensional bar code
or the like (22), and integrated in the part of the identification
card. A text message can be added to a signal before encoding

(30), and the text message can also be printed in the

identification card as a sentence. For example, a signal

indicating a an image is enciphered by using a public key

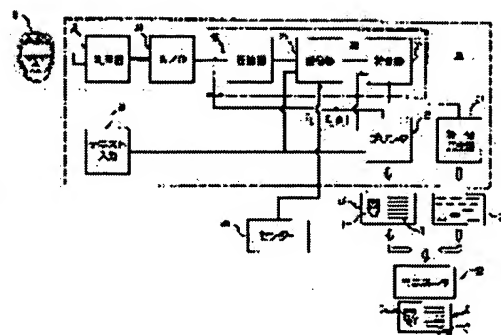
encipherment system, and the key is always changed for

improving safety. A corresponding decoding key is enciphered

by another key, and integrated into the card for easily attaining

certification. The encoded message is scanned, decoded,

extended, displayed, and compared with the image and text message printed in the card for
confirming the validity of the card so that the card can be certified.



(11)特許出願公開番号

(43)公開日 平成7年(1995)2月7日

1

【特許請求の範囲】

【請求項1】 a) 物その他の実体を走査して、その物その他の実体の画像を表す第1の信号を発生する過程と、
 b) 前記画像を識別カードの第1の部分の上にプリントする過程と、
 c) 前記画像の表現を含み、前記第1の信号から少なくとも部分的に得られる第2の信号を暗号化する過程と、
 d) 前記暗号化された第2の信号の符号化された表現を前記識別カードの第2の部分に組み込む過程と、
 e) 前記第2の信号の前記符号化された表現を前記識別カードから読出す過程と、
 f) 前記第2の信号を復号する過程と、
 g) 前記復号された第2の信号を解説する過程と、
 h) 前記画像の前記表現を表示するために前記解説された第2の信号を表示装置へ入力する過程と、
 i) 前記プリントされた画像を前記表示された第2の画像と比較して前記カードの有効性を確認する過程と、
 j) 前記プリントされた画像を前記物その他の実体と比較してその同一性を確認する過程と、を備える物その他の実体を識別する方法。

【請求項2】 請求項1記載の方法において、前記第1の信号をデジタル信号へ変換する過程を更に備える方法。

【請求項3】 請求項2記載の方法において、前記第2の信号は圧縮された態様の前記第1の信号を含む方法。

【請求項4】 請求項3記載の方法において、公開鍵暗号化システムに対する暗号化鍵、E₁、を用いて前記第2の信号を暗号化する方法。

【請求項5】 請求項4記載の方法において、前記暗号化鍵、E₁、に対応する解読鍵、D₁、を、前記公開鍵暗号化システムに対する第2の暗号化鍵、E₂、で暗号化する方法。

【請求項6】 請求項5記載の方法において、前記暗号化された解読鍵、E₂、[D₁]を、前記第2の部分に組み込む前に、前記暗号化された第2の信号へ付す方法。

【請求項7】 請求項6記載の方法において、前記暗号化された第2の信号の前記表現を二次元バーコードとして前記第2の部分中に組み込む方法。

【請求項8】 請求項6記載の方法において、前記暗号化された第2の信号の解読は、解読鍵D₁を用いて前記暗号化された鍵、E₂、[D₁]を解読する過程を更に備える方法。

【請求項9】 請求項3記載の方法において、前記暗号化された第2の信号の前記表現を二次元バーコードとして前記第2の部分中に組み込む方法。

【請求項10】 請求項2記載の方法において、前記第2の信号はテキスト・メッセージを備える方法。

【請求項11】 請求項10記載の方法において、前記物その他の実体は人であり、前記テキスト・メッセージはその人が知っている暗証である方法。

【請求項12】 請求項10記載の方法において、前記テ

2

キスト・メッセージを平文テキスト形式で前記識別カードの前記第1の部分にプリントする方法。

【請求項13】 a) 物その他の実体を走査して前記物その他の実体の画像を表す第1の信号を生ずる過程と、

b) 前記画像を前記カードの第1の部分の上にプリントする過程と、

c) 前記画像の表現を含み、前記第1の信号から少なくとも部分的に得られる第2の信号を暗号化する過程と、

d) 前記暗号化された第2の信号の符号化された表現を前記識別カードの第2の部分中に組み込む過程と、を備える識別カードを製造する方法。

【請求項14】 請求項13記載の方法において、前記第1の信号をデジタル信号へ変換する過程を更に備える方法。

【請求項15】 請求項14記載の方法において、前記第2の信号は圧縮された態様の前記第1の信号を含む方法。

【請求項16】 請求項15記載の方法において、公開鍵暗号化システムに対する暗号化鍵、E₁、を用いて前記第2の信号を暗号化する方法。

【請求項17】 請求項16記載の方法において、前記暗号化鍵、E₁、に対応する解読鍵、D₁、を、前記公開鍵暗号化システムに対する第2の暗号化鍵、E₂、で暗号化する方法。

【請求項18】 請求項17記載の方法において、前記暗号化された解読鍵、E₂、[D₁]を、前記第2の部分に組み込む前に、前記暗号化された第2の信号へ付す方法。

【請求項19】 請求項18記載の方法において、前記暗号化された第2の信号の前記表現を二次元バーコードとして前記第2の部分に組み込む方法。

【請求項20】 請求項15記載の方法において、前記暗号化された第2の信号の前記表現を二次元バーコードとして前記第2の部分に組み込む方法。

【請求項21】 請求項14記載の方法において、前記第2の信号はテキスト・メッセージを備える方法。

【請求項22】 請求項21記載の方法において、前記物その他の実体は人であり、前記テキスト・メッセージはその人が知っている暗証である方法。

【請求項23】 請求項21記載の方法において、前記テキスト・メッセージを平文テキスト形式で前記識別カードの前記第1の部分にプリントする方法。

【請求項24】 a) 識別カードにより識別すべき物その他の実体の画像を発生するための走査手段と、

b) この走査手段に応答して前記画像を前記識別カードの第1の部分にプリントするプリント手段と、

c) 前記画像の表現を含み、前記第1の信号から少なくとも部分的に得られる第2の信号を暗号化する暗号化手段と、

d) 前記第2の信号の前記暗号化の符号化された表現を

前記識別カードの第2の部分に組み込む符号化手段と、
を備える識別カードを製造する装置。

【請求項25】請求項24記載の装置において、前記第1の信号をデジタル信号へ変換するアナログ-デジタル変換器を更に備える装置。

【請求項26】請求項25記載の装置において、前記第1の信号を圧縮する手段を更に備える装置。

【請求項27】請求項25記載の装置において、公開鍵暗号化システムに対する暗号化鍵、E₁、を用いて前記第2の信号を暗号化する手段を更に備える装置。

【請求項28】請求項27記載の装置において、解説鍵、D₁、が第2の暗号化鍵、E₁、で暗号化され、暗号化された解説鍵、E₁ [D₁] が、前記第2の部分に組み込まれる前に、前記暗号化された第2の信号へ付される装置。

【請求項29】請求項27記載の装置において、前記暗号化された第2の信号の前記表現を二次元バーコードとして前記第2の部分に組み込む手段を更に備える装置。

【請求項30】請求項27記載の装置において、前記暗号化鍵、E₁、と前記暗号化された解説鍵、E₁ [D₁] を中央局から受ける手段を更に備える装置。

【請求項31】請求項26記載の装置において、前記暗号化された第2の信号の前記表現を二次元バーコードとして前記第2の部分に組み込む手段を更に備える装置。

【請求項32】識別すべき物その他の実体の画像を第1の部分の上に有し、組み込まれた前記画像の符号化された表現を第2の部分の上に有する識別カードの有効性を確認する方法であって、

- a) 前記信号の前記符号化された表現を前記カードから読出す過程と、
- b) 前記信号の前記符号化された表現を復号する過程と、
- c) 前記信号の前記暗号化された表現を解説する過程と、
- d) 前記画像の前記表現を表示するための表示器へ前記信号の前記解説された表現を入力する過程と、を備え、それにより、
- e) 前記カードの前記第1の部分における前記画像を、前記画像の表示された表現と比較することにより前記カードの有効性を確認できる識別カードの有効性を確認する方法。

【請求項33】請求項32記載の方法において、公開鍵暗号化システムに対する暗号化鍵、E₁、を用いて前記暗号化された信号を暗号化する方法。

【請求項34】請求項33記載の方法において、前記鍵、E₁、に対応する解説鍵、D₁、を、前記公開鍵暗号化システムに対する第2の暗号化鍵、E₁、で暗号し、前記暗号化された解説鍵、E₁ [D₁] を前記暗号化された信号へ付し、前記解説過程は、

- a) 前記暗号化された解説鍵、E₁ [D₁] を対応する

解説鍵D₁で解説して前記解説鍵、D₁、を回復する過程と、

- b) 前記暗号化された信号を前記鍵、D₁、で解説する過程と、を備える方法。

【請求項35】識別すべき物その他の実体の画像を第1の部分に有し、組み込まれた前記画像の符号化された表現を第2の部分の上に有する識別カードの有効性を確認する装置であって、

- a) 前記信号の前記符号化された表現を前記カードから読出す手段と、
- b) この読出し手段に応答して、前記信号の前記符号化された表現を復号する復号手段と、
- c) この復号手段に応答して、前記信号の前記復号された表現を解説する解説手段と、
- d) この解説手段に応答して、前記画像の前記表現を表示する表示手段と、を備え、それにより、
- e) 前記カードの前記第1の部分における前記画像を、前記画像の表示された表現と比較することにより前記カードの有効性を確認できる識別カードの有効性を確認する装置。

【請求項36】請求項35記載の装置において、公開鍵暗号化システムに対する暗号化鍵、E₁、を用いて前記暗号化された信号が暗号化される装置。

【請求項37】請求項36記載の装置において、前記鍵、E₁、に対応する解説鍵、D₁、が、前記公開鍵暗号化システムに対する暗号化鍵E₁で暗号化されて、暗号化された解説鍵、E₁ [D₁] を形成し、前記暗号化された解説鍵、E₁ [D₁] を前記暗号化された信号へ付し、前記解説手段は、

- a) 前記暗号化された解説鍵、E₁ [D₁] を対応する解説鍵D₁で解説して前記解説鍵、D₁、を回復する手段と、
- b) 前記暗号化された信号を前記鍵、D₁、で解説する手段と、を備える装置。

【請求項38】識別カードであって、この識別カードは、

- a) 前記識別カードにより識別すべき物その他の実体の画像を有する第1の部分と、
- b) 前記画像の表現を含む暗号化された信号の符号化された表現を組み込む第2の部分と、を備える識別カード。

【請求項39】請求項38記載の識別カードにおいて、前記信号はデジタル信号である識別カード。

【請求項40】請求項39記載の識別カードにおいて、前記デジタル信号は、前記物その他の実態を走査することにより発生された走査信号から得られる圧縮された信号を備える識別カード。

【請求項41】請求項40記載の識別カードにおいて、公開鍵暗号化システムに対する暗号化鍵、E₁、を用いて前記デジタル信号が暗号化される識別カード。

【請求項42】請求項41記載の識別カードにおいて、前記暗号化鍵、E₁、に対応する解読鍵、D₁、が、前記公開鍵暗号化システムに対する暗号化鍵E₁で暗号化されて、暗号化された解読鍵、E₁ [D₁]を形成し、前記暗号化された解読鍵、E₁ [D₁]は、前記第2の部分へ組み込む前に、前記デジタル信号へ付される識別カード。

【請求項43】請求項42記載の識別カードにおいて、前記暗号化されたデジタル信号の前記表現は二次元バーコードとして前記第2の部分に組み込まれる識別カード。

【請求項44】請求項40記載の識別カードにおいて、前記暗号化されたデジタル信号は二次元バーコードとして前記第2の部分に組み込まれる識別カード。

【請求項45】請求項39記載の識別カードにおいて、前記デジタル信号はテキスト・メッセージを備える識別カード方法。

【請求項46】請求項45記載の識別カードにおいて、前記物その他の実体は人であり、前記テキスト・メッセージはその人が知っている暗証である識別カード。

【請求項47】請求項45記載の識別カードにおいて、前記テキスト・メッセージは前記識別カードの前記第1の部分の上の平文テキスト形式である識別カード。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、物その他の実体の同一性または状態の証拠として機能する識別カードまたはそれに類似の物品に関するものである。更に詳しく言えば、本発明は、偽造または変造に対して高度の安全性を有する識別カードまたは類似の物品と、それらのカードの製造及び認証方法および装置に関するものである。

【0002】（この明細書で使用する「識別カード」という用語は、従業員を識別するために事業所により用いられる種類の識別バッジに類似する物を指すものであるが、文書、磁気ディスク、CD等、または関連するデータと共に画像を記録でき、かつ識別すべき物その他の実体に関連させることができるその他の任意の適当な物を、ここで使用する「識別カード」という用語が限定なしに含むべきことが、本発明の意図に含まれる。）物その他の実体の識別は少なくとも歴史のように古い問題である。年取って盲目になったイサクは、エサウの相統棒に頼ってエサウをヤコブから見分けることに失敗し、ソロモンは赤子の母親を見つけるためにその赤子を殺すと脅かす事を余儀なくされた。歴史および物語は、所持している人を識別するために用いられる手紙、しるし、玉璽および暗証と、それらが失われ、または偽造された後に続く結末についての話に満ちている。

【0003】現代においては、この問題についての最もありふれた解決は、所有者の同一性と、所有者の通常はある特徴、状態、または属性を定める機能を果たす識別

カードである。その例は上記のように従業員バッジであり、最も一般的には運転免許証である。典型的には、そのような識別カードは公称所有者の写真と、文書形式の関連する情報を含む。

【0004】識別カードなどは毎日の管理業務に有用であることが一般に判明しているが、それでも、識別カードは偽造または変造されることがあり、偽の識別文書を供給する目的の適度な規模の非合法事業が存在する。

【0005】識別についての高度の安全性が要求される用途に対しては、指紋、声紋、網膜模様、その他の個人的な特徴を認識するための効率的な技術が開発されている。そのようなシステムはシステムが知っている個人を一意に識別するには極めて成功しているが、選択された個人を指紋のような身体的特徴で識別するデータベースへ接続せねばならない、典型的には可動ではない、極めて高性能の、極めて高価なセンサを必要とすることが欠点である。不法な変更に対する保護と更新を容易にするために、そのようなデータベースは一般に中央に設置せねばならない。したがって、それらの高度なシステムは区域を安全にするために接近を制約することに一般に限定される。

【0006】以上の説明から明らかなように、識別カードの最も一般的な用途は個人識別である。しかし、識別の目的は非常に広い種類の物その他の実体に拡張できる。したがって、特定の項目が検査された、または税関を通過した、あるいは特定の会社により製造された、ことを確認できることが望ましい。同様に、美術工芸品の出所、動物の血統または人の家系、あるいは植物が病原菌に犯されていないこと、の確実な証拠を持つことが望ましい。そのような用途、および当業者には明らかであるその他の用途は本発明の範囲内である。

【0007】おそらく有体物ではなくて情報に関連するからであろう、文書その他の態様の情報の識別すなわち認証が過去において、通常はある種の暗号化を使用することにより、多分成功裡に取り扱われてきた。したがって、1989年8月1日にパストー（Pastor）へ付与された米国特許第4,853,961号「信頼できる文書認証装置（Reliable Document Authentication System）」には、公開鍵暗号方式を用いる暗号化により文書を認証する装置が開示されている。クラーク（Clark）へ付与された米国特許第4,637,051号には、暗号化により認証される標識を持つ郵便料金計が開示されている。情報を認証するための暗号化のその他の多くの用途が当業者には知られていることであろう。

【0008】

【発明が解決しようとする課題】したがって、本発明の目的は、変造および偽造に対して安全である、物その他の実体を識別するための識別カードを得ることである。

【0009】

【課題を解決するための手段】識別カードを製造する方法および装置、およびその識別カードの有効性を確認する方法および装置を提供する本発明により上記目的は達成され、かつ従来技術の諸欠点が克服される。識別カードを製造する装置は、識別すべき物その他の実体の画像を表す第1の信号を発生する走査器と、この走査器にตอบสนองして画像を識別カードの第1の部分の上にプリントするプリンタとを含む。この装置は、画像の表現を含み、第1の信号から少なくとも部分的に得られる第2の信号を暗号化する暗号化器と、第2の信号の暗号化の符号化された表現を識別カードの第2の部分に組み込む符号器とを更に含む。

【0010】そのようにして製造された識別カードの有効性を確認する装置は、第2の信号の符号化された表現をカードから読出す読出し器と、この読出し器の第2の信号の符号化された表現を復号する復号器と、復号された表現を解読する解読器と、第2の信号に組み込まれている画像の表現を表示する表示器とを含む。

【0011】本発明の方法に従って、識別すべき物が走査されて第1の信号を発生し、第1の信号により制御されるプリンタがその物の画像を識別カードの第1の部分の上にプリントする。第1の信号から少なくとも部分的に得られ、画像の表現を含む第2の信号を暗号化および符号化し、識別カードの第2の部分に組み込む。

【0012】ひとたび製造されたカードは、第2の信号の符号化された表現を識別カードから読出し、解読された第2の信号に従って表示装置を制御して、第2の信号に含まれている画像の表現を表示する。それから画像の表示された表現およびカードの第1の部分にプリントされた画像を物と比較してその同一性を確認する。

【0013】本発明の1つの面に従って、第1の信号は処理のためにデジタル信号へ変換される。

【0014】本発明の別の面に従って、第2の信号は圧縮された態様の第1の信号を含む。

【0015】(信号圧縮は当業者に周知であって、デジタル信号の場合には、伝送または処理せねばならないバイト数を減少し、しかもその信号により表されている情報のほとんど全てを依然として保持するために、信号に対する所定のアルゴリズムの適用を含む。) 本発明の別の面に従って、第2の信号は公開鍵暗号化システムに対する暗号化鍵E₁を用いて暗号化される。

【0016】本発明の別の面に従って、暗号化鍵、E₁、に対応する解読鍵、D₁、を、公開鍵暗号化システムに対する第2の暗号化鍵、E₂、で暗号化し、結果としての暗号化された解読鍵、E₁ [D₁] を、第2の部分に組み込む前に、暗号化された第2の信号へ付す。

【0017】本発明の別の面に従って、暗号化された第2の信号を二次元バーコードとして識別カードの第2の部分にプリントする。

【0018】本発明の別の面に従って、識別カードの有

効性を識別する装置は鍵E₂に対応する解読鍵、D₂を記憶し、暗号化された第2の信号の解読は、暗号化された解読鍵、E₁ [D₁] を、解読鍵、D₂を用いて解読して解読鍵D₁を得、それから暗号化された第2の信号をその解読鍵を用いて解読する過程を含む。

【0019】本発明の別の面に従って、第2の信号はテキスト・メッセージを含み、そのテキスト・メッセージは識別カードにより識別すべき人が知っている暗証を含む。

【0020】本発明の更に別の面に従って、第2の信号はテキスト・メッセージを含み、そのテキスト・メッセージは識別カードの第1の部分に平文形式でプリントもされる。

【0021】したがって、本発明は、同一性を確認すべき物その他の実体と容易に比較でき、かつ偽造または変造に強い画像を含む識別カードを製造する方法および装置により、上記目的を達成するものであることがわかる。

【0022】

【実施例】図1は識別カードCを製造するための装置10の概略ブロック図を示す。識別カードが意図されている人(または物その他の実体)が通常のテレビカメラ12により走査されて、その人の画像を表す第1の信号を発生する。それから、第1の信号をデジタル領域で処理するためにアナログーデジタル変換器14によりデジタル形式へ変換することが好ましい。しかし、以下に説明する少なくとも信号圧縮技術および暗号化技術を、アナログ信号処理技術における当業者に周知の信号圧縮技術および信号暗号化技術を用いてアナログ領域において実施できる。

【0023】それから、第1の信号は圧縮モジュール16へ入力され、そこで圧縮されて、識別カードに記憶せねばならないデータの量を減少する。

【0024】カードCが現在知られている識別カード、運転免許証などとほぼ同じ形式を持つ場合には、現在の技術状態においてはデータ圧縮を必要とすることに注目すべきである。しかし、データ記憶技術における予測される改良により、または識別カードが高い容量の記憶媒体(たとえば、フロッピーディスク)を含むことができる用途においては、後で述べるように第1の信号を圧縮する必要がないが、完全な信号を処理できることも本発明の範囲内である。

【0025】データ圧縮アルゴリズム、とくにビデオ画像信号の圧縮に用いられるデータ圧縮アルゴリズム、は当業者に周知である。市販されているJPEGアルゴリズムとして知られているアルゴリズムを圧縮器16に用いることが好ましい。圧縮器16の動作の動作についてのこれ以上の説明は本発明の理解には不必要であると信ぜられる。

【0026】それから圧縮された第1の信号は暗号器2

0へ入力されて、暗号化された第2の信号に含まれる。その暗号化された第2の信号は、後で説明するように、識別カードCに組み込まれる。暗号器20は周知のRSA方式のような公開鍵暗号方式のための暗号化鍵、E₁、を用いて第2の信号を暗号化することが好ましい。

【0027】それから暗号化された第2の信号は符号器モジュール22によりある所定のフォーマットに従って符号化される。それは符号発生器24を制御して符号化されて暗号化された第2の信号を識別カードCの部分中

に組み込ませる。
【0028】本発明の好適な実施例に従って、符号化された信号は、ニューヨーク所在のシンボル・テクノロジー・コーポレーション (Symbol Technology Corporation) により開発されたPDF-417標準バーコードのような、二次元バーコードとして符号化される。しかし、暗号化された第2の信号は適当な任意のフォーマットへ符号化できる。たとえば、スマートカードまたは記憶カードに対して符号器22およびコード発生器24は符号化された第2の信号を適切にフォーマット化された2進データ・ブロックとして記憶できる。

【0029】符号化された第2の信号が二次元バーコードとして表される好適な実施例においては、バーコードは識別カードCの裏面CBにプリントすることが好ましい。

【0030】本発明の好適な実施例においては、圧縮器モジュール16と、暗号器モジュール20と、符号器モジュール22とはマイクロプロセッサにおけるソフトウェア・モジュールとして実現される。そのマイクロプロセッサはインテル80386型、またはそれと同等品、あるいはより高い性能のマイクロプロセッサであることが好ましい。

【0031】デジタル化された第1の信号はプリンタ20へも入力される。そのプリンタは、人目の画像を識別カードCの表面CFにプリントするために識別カードCを製造する任意の適切な技術を使用できる。それから表面CFと裏面CBを組み合わせ、ラミネータ32により周知の技術を用いてラミネートして識別カードCを製造する。

【0032】本発明の別の好適な実施例に従って、テキスト・メッセージを入力するためにテキスト入力部30が用いられる。本発明の一実施例においては、テキスト・メッセージの少なくとも一部が圧縮された態様の第1の信号に組合わされて第2の信号を形成する。その第2の信号は暗号器モジュール20により暗号化され、かつカードCの表面CFに平文テキストとしてプリントもされる。あるいは、テキスト・メッセージTを、たとえば、制御キャラクタの削除により圧縮できる。それらのキャラクタは、テキスト・メッセージTが第2の信号へ

組み込まれる前に、テキストTが回収された時に、所定のフォーマットに従って回復される。したがって、画像1のようにテキスト・メッセージTは、カードCの表面CFに人が認識できる形式で、および裏面CBに符号化された形式でカードCに具体化される。別の実施例においては、テキスト・メッセージは暗証Pを含むことができる。その暗証は暗号化され、かつ符号化されるが、表面CFには平文でプリントされない。

【0033】本発明の好適な実施例においては、センター40が暗号化鍵E₁を暗号器モジュール20へ送る。識別カードCの安全性を高くするために、鍵E₁を始終変更する。鍵E₁の安全度を最高にするためには、各カードCを製造するたびに鍵を変更し、または第2の信号の種々の部分を暗号化するために異なる鍵を使用することもできる。

【0034】鍵E₁がしばしば変更される環境における第2の信号の暗号化を容易にするために、センター40は暗号化された解読鍵E₁ [D₁]を送って符号器モジュール22により暗号化された第2の信号へ付させる。このように、下でわかるように、カードCの有効性を確認する時に、E₁ [D₁]を解読することにより必要な解読鍵D₁を得ることができる。

【0035】典型的には、暗号化鍵/解読鍵対E₁、D₁は装置10が動作中はほぼ一定のままである。しかし、各種の組織のための識別カードCを製造するために装置10が使用される用途においては、種々の鍵対E₁、D₁を種々の組織のために使用できる。

【0036】次に、識別カードCの有効性を確認するための装置50が示されている図2を参照する。カードCの裏面CBが、適切な二次元バーコードを走査できる性能を有するバーコード走査器52により走査される。本発明の好適な実施例においては、解読鍵D₁を得るために暗号化されている解読鍵E₁ [D₁]を解読するために用いられる解読鍵D₁を解読器58が保存する。それから鍵D₁を用いて、カードの裏面CBから走査される復号された信号を解読する。

【0037】鍵D₁はセンター40から解読器58により得られる。典型的には、上記のように、装置50の動作中は鍵D₁は一定に保たれ、装置50とセンター40の間の直接通信リンクは不必要であり、鍵D₁は任意の便利なやり方で送ることができる。しかし、識別カードCが所定の満期期限を有するある用途においては、その満期期限の経過後は鍵D₁を変更することが望ましく、そのような満期期限が十分にしばしば生ずるものとする、センター40への直接通信リンクを装置50に含むことができる。

【0038】それから、解読された走査信号は装置10において使用される圧縮アルゴリズムに対して相補的なアルゴリズムにより、通常のやり方で拡張される。本発明の理解のためにはそのやり方を説明する必要はない。

【0039】本発明の好適な実施例においては、復号器モジュール54と、解読器モジュール58と、拡張器モジュール60とをマイクロプロセッサ61においてソフトウェア・モジュールとして実現できる。

【0040】解読され、拡張された信号がそれから通常の表示装置62により表示される。表示装置は画像Tの表現RIと、カードの裏面CBから走査される暗号化された第2の信号に含まれていたテキスト・メッセージTを含む。表示装置は暗証Pを含む。その暗証はカードCを所持することを許されている人Oに知られているが、上記のようにカードCには含まれない。カードの有効性を確認するために、画像Iがその表現RIと比較され、カードCにプリントされていて、表示装置62に示されているテキスト・メッセージTが比較される。圧縮により表現RIが画像Iに対して多少劣化させられることに注目すべきである。しかし、上記JPEGアルゴリズムを使用すると、人の顔の画像の十分に正確な表現をデータの約1000バイトとして符号化でき、ほぼ従来の札入れ寸法のカードの裏面に約6.35×4.45cm(約2.50×1.75インチ)の区域に上記PDF-417二次元バーコードを用いてプリントできる。もちろん、上記のように、記憶装置技術の改良と、より大きいデータ記憶容量を有する媒体の使用との少なくとも一方により、識別カードCの表現RIの実施例を画像Iへ任意に近づけることができる。

【0041】暗証Pを含む実施例においては、暗証Pは表示装置62の上に示されるが、カードの表面CFにはもちろんプリントされない。暗証PはカードCを所持する事を許されている人Oは知っている。画像Iと、カードの表面CFにプリントされているテキスト・メッセージTを、表示装置62に示されている表現RIとテキス

ト・メッセージTと比較することにより有効であることが確認されると、カードCを所持している人Oと画像Iを比較し、かつ暗証Pを知っているかどうかその人Oを試すことにより、その人を確認できる。それからテキスト・メッセージTはその人Oの同一性を確認し、かつその人Oの状態または特徴も確認できる。

【図面の簡単な説明】

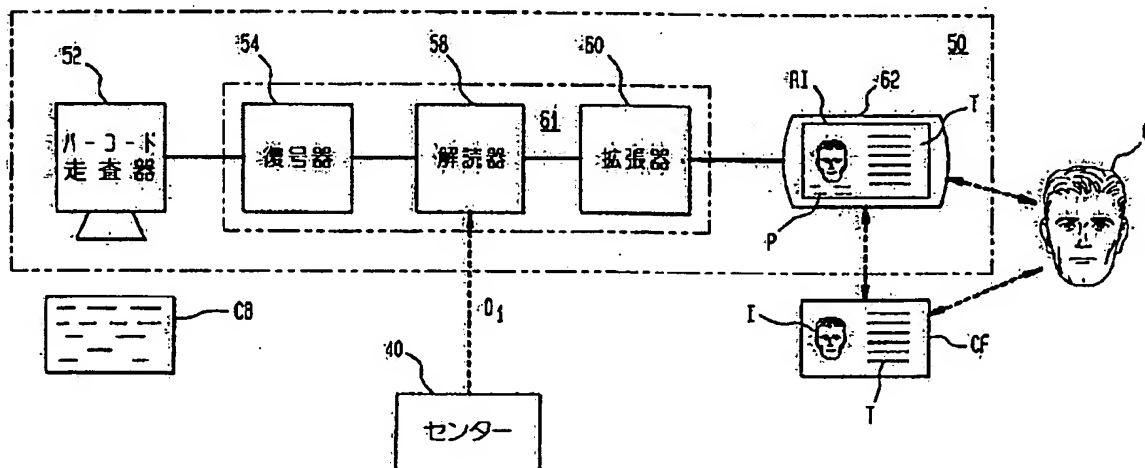
【図1】本発明に従って識別カードを製造する装置の概略ブロック図である。

【図2】本発明に従って製造された識別カードの有効性を確認する装置の概略ブロック図である。

【符号の説明】

- 10 識別カードを製造する装置
- 12 走査器
- 14 アナログデジタル変換器
- 16 圧縮器
- 20 暗号器
- 22 符号器
- 24 符号発生器
- 28 プリンタ
- 30 テキスト入力部
- 32 ラミネータ
- 46 センター
- 50 識別カードの有効性を確認する装置
- 52 バーコード走査器
- 54 復号器
- 58 解読器
- 60 拡張器
- 61 マイクロプロセッサ
- 62 表示装置

【図2】



【図1】

